

Amendment #1
Request for Proposals # 09-26-001
State Asset Servicing System

The purpose of this Amendment is to amend and clarify certain information contained in the above named Request for Proposals (RFP). All information contained herein is binding on all offerors who respond to this RFP as provided for in Section 1.15 of the above named RFP. The Closing Date and Time and specific parts of the RFP have been amended.

The following changes/additions are listed below; new language has been underlined and marked in bold (i.e., **word**) and deleted language has been marked with a strikeout (i.e., ~~word~~).

1. Extend Closing Date and Time:

Closing Date and Time: ~~December 3, 2008 2:00 pm local time~~ **December 22, 2008 5:00 pm local time.**

2. Revise Section 3.2.B System Requirements:

1. Operating System and Development Platform.

- a. Run on a Microsoft Windows Server 2003 ~~operating~~ **network environment.**
- b. Use **a relational database platform, preferably** Microsoft SQL Server, version 2005 or later, ~~as the database platform.~~

3. Revise Section 5.2.B Technical Proposal:


Tab 4 – Proposed Solution and Approach:

- 14. Hosted solutions - external network connection security measures to be instituted in compliance with Exhibit V, Service Interface Agreement Policy.**

4. Add Exhibit V, Service Interface Agreement Policy (attached as page 2 of Amendment #1)

Date Issued: November 20, 2008

By:


Susan Traylor
Procurement Officer

Service Interface Agreement Policy

External network connections shall be permitted only after all approvals are obtained consistent with this policy and shall be managed in accordance with a Service Interface Agreement (SIA) that is agreed to by the State agency and the non-State entity. These connections are subject to the Maryland Public Information Act and should not be part of the ordinary process of doing business. An SIA shall include:

1. Purpose and duration of the connection as stated in the agreement, lease, or contract;
2. Points-of-contact and cognizant officials for both the State and non-State organizations;
3. Roles and responsibilities of points-of-contact and cognizant officials for both State and non-State organizations;
4. Security measures to be implemented by the non-State organization to protect the State's IT assets against unauthorized use or exploitation of the external network connection;
5. Requirements for notifying a specified State official within a specified period of time of a security incident on the network, with the recommended time within 4 hours of the incident;
6. A provision allowing the State to periodically test the ability to penetrate the non-State network through the external network connection or system.